Overview of Public-Key Infrastructure

First ITU-T X.509 day

9 May 2022

Erik Andersen

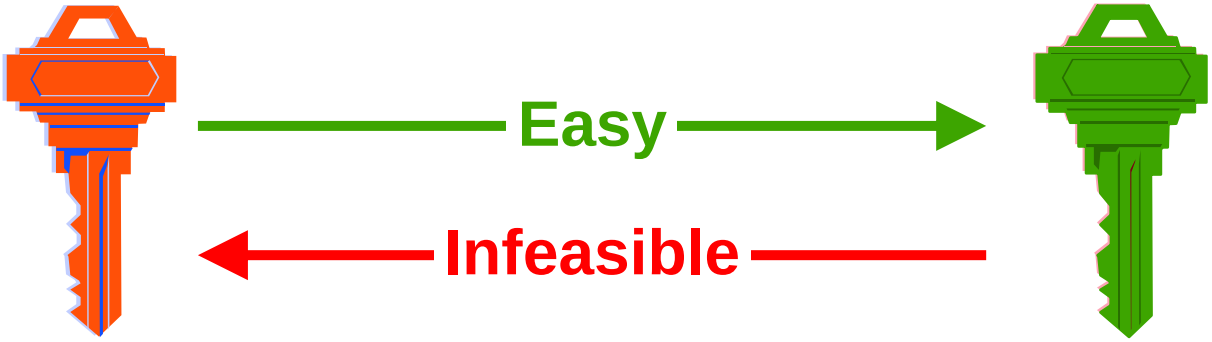
era@x500.eu

Public-key cryptography

In public-key cryptography there are two mathematically related cryptographic keys

Private key (kept protected)

Public key (publicly available)



Currently used algorithms:

- **RSA (Rivest-Shamir-Adelman)**
- **Elliptic curve based cryptographic (ECDSA & EdDSA)**

Public-key cryptography

Public-key cryptography

Is also called

asymmetric cryptography

in contrast to

symmetric cryptography,
e.g., used for encryption like
Advanced Encryption Standard (AES)

Symmetric cryptography vs. Asymmetric cryptography

Two communication entities:

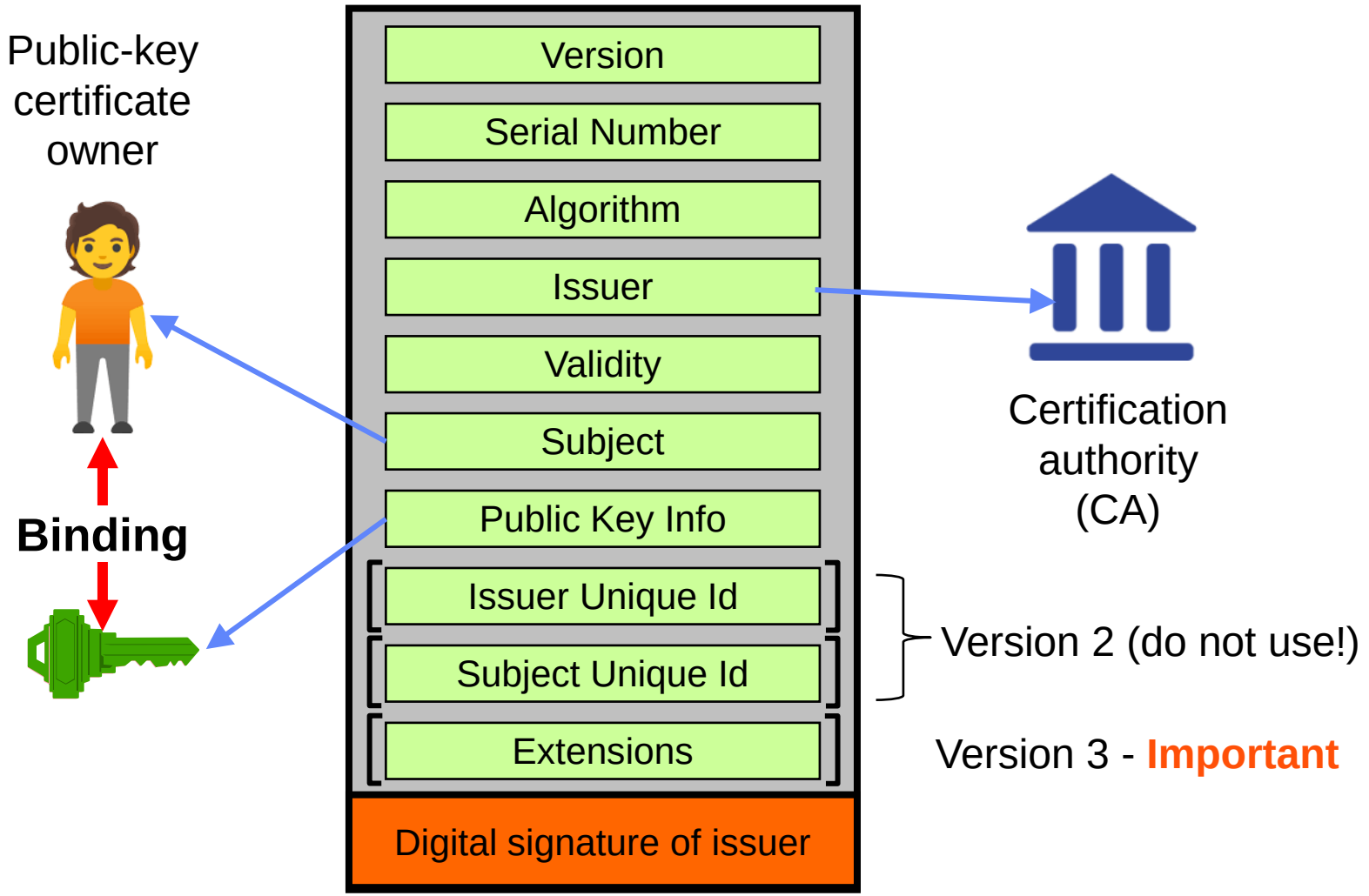
- **Symmetric cryptography:**
  - **Same key used by both communicating entities, e.g., for encryption and decryption**
- **Asymmetric cryptography:**
  - **One entity uses its private key, e.g., to create a digital signature**
  - **The other entity uses the public key of its communication partner to verify the signature**

Digital signature

- A digital signature is bound to the document being signed
- If the document changes, a new changed signature must generated
- If the document is changed after being signed, the verification will fail
- In contrast to handwritten signature

Provides integrity in addition to authentication

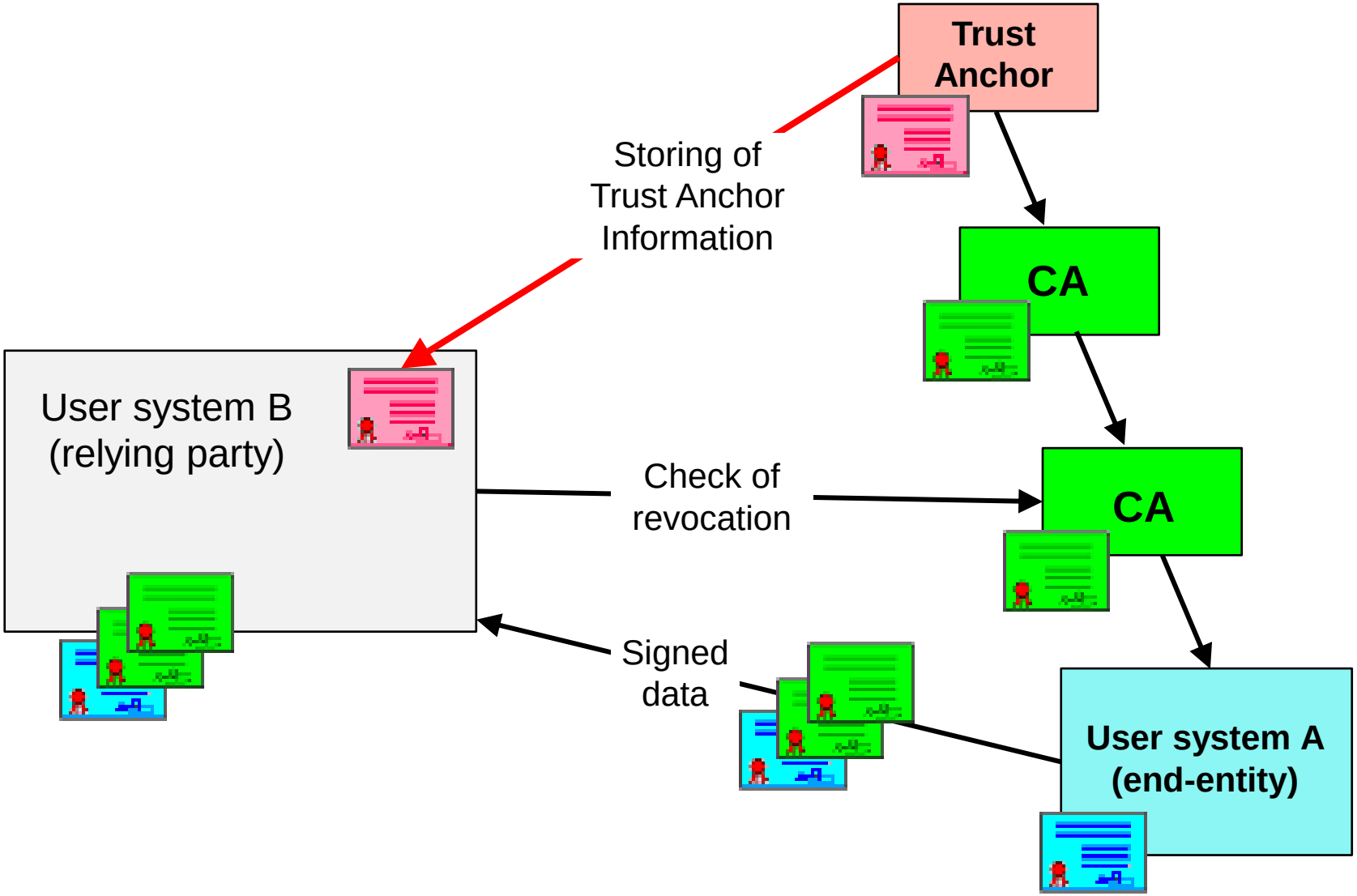
Public-key certificate



Public-key infrastructure (PKI)

A public-key infrastructure (PKI) is a set of policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke public-key certificates

PKI Components

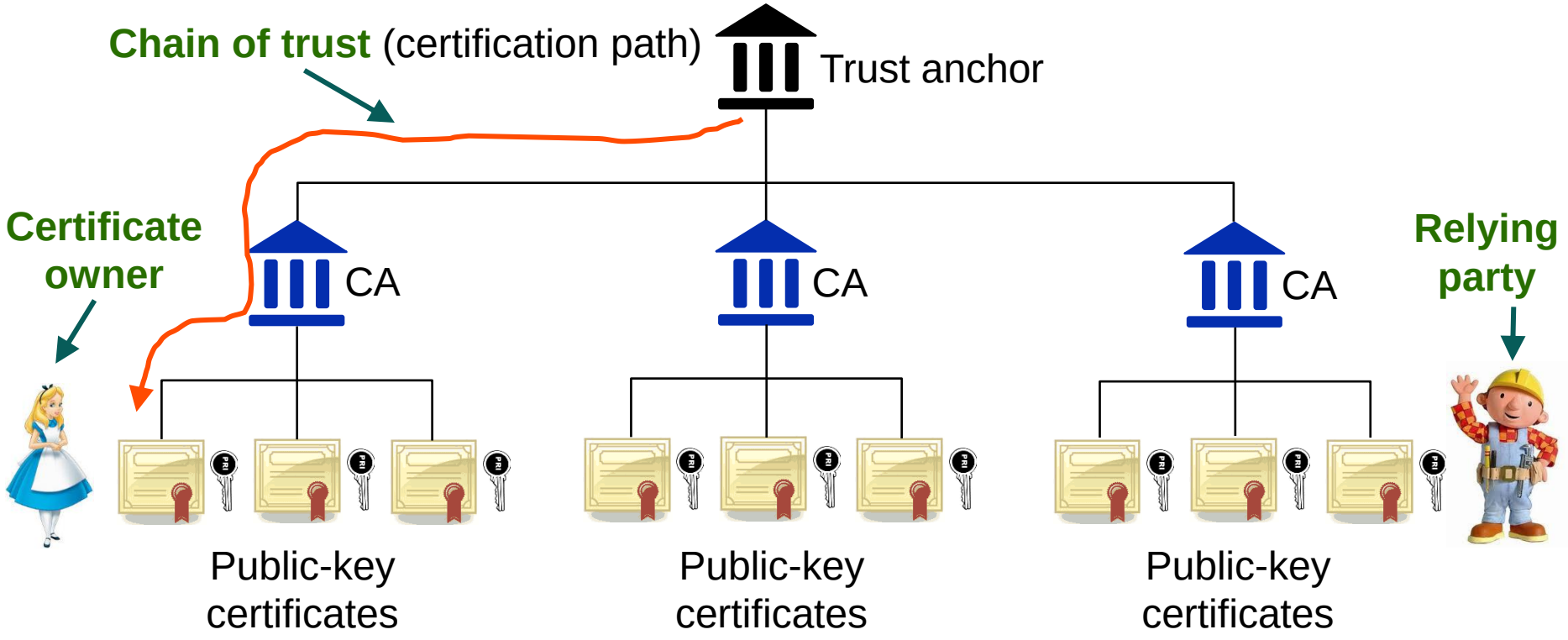


Samples of IETF RFCs supporting PKI

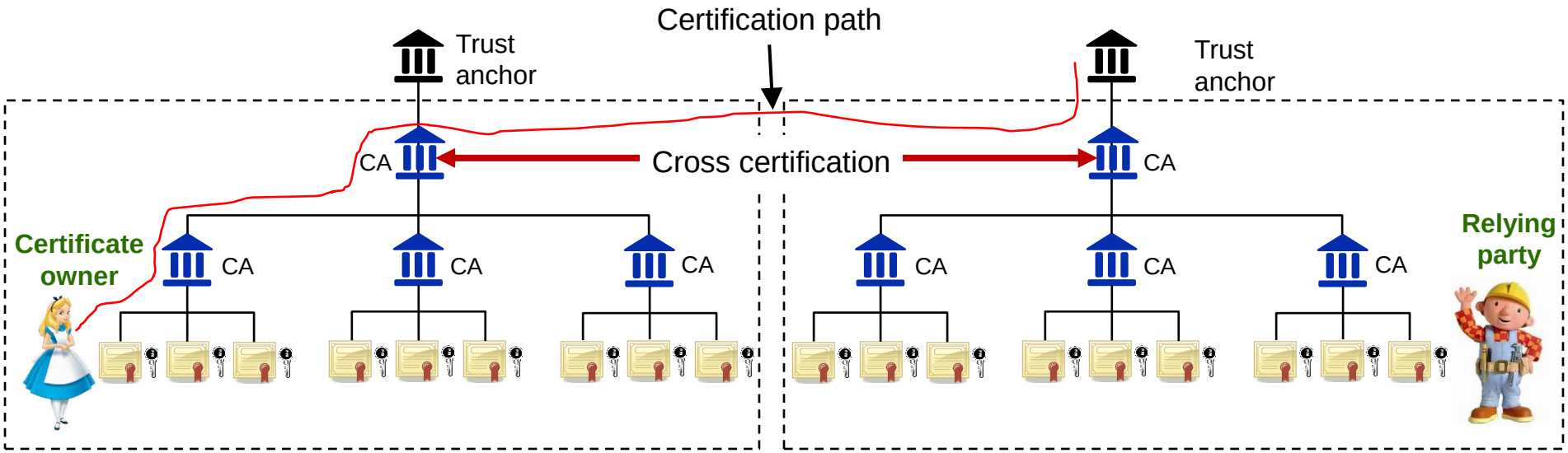
- IETF RFC 2986, PKCS #10: Certification Request Syntax Specification, Version 1.7
- IETF RFC 4210, Internet X.509 Public Key Infrastructure, Certificate Management Protocol (CMP)
- ETF RFC 5272, Certificate Management over CMS (CMC)
- IETF RFC 5934, Trust Anchor Management Protocol (TAMP)
- IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- Several IETF RFCs about cryptographic algorithm

Chain of trust within traditional public-key infrastructure (PKI)

PKI Domain:



Public-key infrastructure (PKI) cross certification



Symmetric key establishment
Another use of public-key cryptography

Two communication entities:

- **Key transport:**
  - **Symmetric key generated by one entity and encrypted using asymmetric encryption or key encapsulation for transport to the other entity**
- **Key agreement:**
  - **Key established by e.g., using Diffie-Helman key exchange**

Key management